CLAIMS

1. A multi-tiered management architecture comprising:

an application development tier at which applications are developed for execution on one or more computers;

an application operations tier at which execution of the applications is managed; and

a cluster operations tier to manage the operation of the computers without concern for what applications are executing on the one or more computers.

2. A management architecture as recited in claim 1, wherein the cluster operations tier is responsible for securing a computer cluster boundary to prevent a plurality of other computers that are not part of the computer cluster from accessing the one or more computers in the computer cluster.

3. A management architecture as recited in claim 1, wherein the application operations tier is responsible for securing sub-boundaries within the computer cluster boundary to restrict communication between computers within the computer cluster.

4. A management architecture as recited in claim 1, wherein the application operations tier is implemented at an application operations management console at a location remote from the one or more computers.

5. A management architecture as recited in claim 1, wherein the cluster operations tier is implemented at a cluster operations management console located at the same location as the one or more computers.

6. A management architecture as recited in claim 1, wherein the application operations tier monitors execution of application processes on the one or more computers and detects failures of the application processes.

7. A management architecture as recited in claim 1, wherein the application operations tier takes corrective action in response to a software failure on one of the computers.

8. A management architecture as recited in claim 7, wherein the corrective action comprises re-booting the computer.

9. A management architecture as recited in claim 7, wherein the corrective action comprises notifying an administrator of the failure.

10. A management architecture as recited in claim 1, wherein the cluster operations tier monitors hardware operation of the one or more computers and detects failures of the hardware.

11. A management architecture as recited in claim 1, wherein the cluster operations tier takes corrective action in response to a hardware failure of one of the computers.

12. A management architecture as recited in claim 11, wherein the corrective action comprises re-booting the computer.

13. A management architecture as recited in claim 11, wherein the corrective action comprises notifying a co-location facility administrator.

14. A management architecture as recited in claim 11, wherein the one or more computers are situated in one or more clusters at a co-location facility.

15. A co-location facility system comprising:

a plurality of node clusters each corresponding to a different customer; and

a cluster operations management console corresponding to at least one of the node clusters and configured to manage hardware operations of the at least one node cluster.

16. A system as recited in claim 15, further comprising a different cluster operations management console corresponding to each of the plurality of node clusters.

17. A system as recited in claim 15, wherein each of the plurality of node clusters includes, as its nodes, a plurality of server computers.

18. A system as recited in claim 15, wherein the hardware operations include one or more of: mass storage device operation, memory device operation, and network interface operation, and processor operation.

19. A system as recited in claim 15, wherein each of the plurality of node clusters includes a plurality of nodes configured to receive node control commands from an application operations management console located remotely from the co-location facility.

20. A system as recited in claim 19, wherein each node in each node cluster is configured with a private key that allows the node to decrypt communications that are received, in a form encrypted using a public key, from the application operations management console associated with the customer that corresponds to the node cluster.

21. A system as recited in claim 15, further comprising a data transport medium coupled to each node in the plurality of clusters via which each node can access an external network.

22. A system as recited in claim 15, wherein the external network comprises the Internet.

23. A system as recited in claim 15, wherein each node in each node cluster is configured with the boundary of the node cluster.

24. A system as recited in claim 15, wherein each node in each node cluster is configured with a private key that allows the node to decrypt communications that are received, in a form encrypted using a public key, from the cluster operations management console.

25. A system as recited in claim 15, wherein one or more of the nodes in a node cluster are leased by the customer from an operator of the co-location facility.

26. A method comprising:

monitoring, at a co-location facility, hardware operations of a cluster of computers located at the co-location facility;

detecting a hardware failure in one of the computers in the cluster; and

performing an act, in response to detecting the hardware failure, to correct the hardware failure.

27. A method as recited in claim 26, wherein the cluster of computers is one of a plurality of clusters of computers located at the co-location facility.

28. A method as recited in claim 26, wherein the act comprises notifying a co-location facility administrator of the failure.

29. A method as recited in claim 26, wherein the act comprises resetting the computer that includes the hardware that failed.

30. A method as recited in claim 26, wherein the hardware operation includes one or more of: mass storage device operation, memory device operation, and network interface operation, and processor operation.

31. A method as recited in claim 26, further comprising configuring each computer in the cluster to impose boundaries preventing a plurality of other computers that are not part of the cluster from accessing the one or more computers in the cluster.

32. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 26.

33. A method comprising:

monitoring, from a location remote from a co-location facility, software operations of a cluster of computers located at the co-location facility;

detecting a software failure in one of the computers in the cluster; and

performing an act, in response to detecting the software failure, to correct the hardware failure.

34. A method as recited in claim 33, wherein the cluster of computers is one of a plurality of clusters of computers located at a co-location facility.

35. A method as recited in claim 33, wherein the act comprises notifying an administrator of the failure.

36. A method as recited in claim 33, wherein the act comprises resetting the computer that executes the software that failed.

37. A method as recited in claim 33, further comprising configuring one or more computers in the cluster to impose sub-boundaries preventing a first one or more computers within the cluster from accessing a second one or more computers within the cluster.

38. A method as recited in claim 33, further comprising managing loading of a software component on one of the computers in the cluster.

39. A method as recited in claim 33, wherein the software failure comprises one or more of: a hung application process, a hung thread, and an error in execution of an application process.

40. A computer, located remotely from the cluster of computers, to implement the method of claim 33.

41. A method as recited in claim 33, wherein the monitoring, detecting, and performing are implemented in a remote computer, and further comprising using public key cryptography to securely communicate between the remote computer and each computer in the cluster of computers.

42. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 33.

43. One or more computer-readable media having stored thereon a computer program that, when executed by one or more processors, causes the one or more processors to perform acts including:

monitoring, from a location remote from a co-location facility, software operations of a cluster of computers located at the co-location facility; and

taking corrective action in response to a failure in operation of software executing on one of the computers in the cluster.

44. One or more computer-readable media as recited in claim 43, wherein the corrective action comprises notifying an administrator of the failure.

45. One or more computer-readable media as recited in claim 43, wherein the corrective action comprises resetting the computer that executes the software that failed.

46. One or more computer-readable media as recited in claim 43, wherein the computer program, when executed, further causes the one or more processors to perform acts including configuring each computer in the cluster to impose boundaries preventing a plurality of other computers that are not part of the cluster from accessing the one or more computers in the cluster.

47. One or more computer-readable media as recited in claim 43, wherein the failure in operation of the software comprises one or more of: a hung application process, a hung thread, and an error in execution of an application process.

48. A method comprising:

selling, to a customer, rights to a plurality of computers to be located at a facility; and

enforcing a multiple-tiered management scheme on the plurality of computers in which hardware operation of the plurality of computers is managed locally at the facility and software operation of the plurality of computers is managed from a location remote from the facility.

49. A method as recited in claim 48, wherein the facility comprises a co-location facility.

50. A method as recited in claim 48, wherein the selling comprises licensing at least one of the plurality of computers to the customer.

51. A method as recited in claim 48, wherein the selling comprises selling at least one of the plurality of computers to the customer.

52. A method comprising:

allowing a tenant to which a cluster of one or more computers at a facility have been leased to communicate with the one or more computers; and

implementing cluster boundaries at the facility to prevent computers within the cluster from communicating with computers in another cluster.

53. A method as recited in claim 52, wherein the facility comprises a co-location facility.

54. A method as recited in claim 52, wherein the allowing comprises establishing secure communications channels between the one or more computers and a corresponding tenant operations management console.

55. A method as recited in claim 54, wherein:

the cluster boundaries are implemented at a first tier of a multi-tiered management architecture; and

allowing the tenant operations management console, implemented in a second tier of the multi-tiered management architecture, to establish sub-boundaries within the cluster.

56. A method as recited in claim 52, further comprising:

performing at least some management of the computers via a landlord operations management console; and

establishing secure communications channels between each of the plurality of computers and the landlord operations management console.

57. A method as recited in claim 56, wherein the landlord operations management console is located at the facility.

58. A method as recited in claim 52, wherein the cluster includes one or more additional computers that have not been leased to the tenant.

59. A method comprising:

separating a plurality of computers at a co-location facility into a plurality of clusters;

leasing the clusters to a plurality of tenants; and

allowing secure communications channels to be established between the computers in the cluster leased to the tenant and an operations management console of the tenant.

60. A method as recited in claim 59, further comprising:

performing at least some management of the computers via a landlord operations management console; and

allowing secure communications channels to be established between the computers in the cluster leased to the tenant and the landlord operations management console.

61. A method as recited in claim 59, further comprising implementing cluster boundaries to prevent computers within a cluster from communicating with computers in another cluster.

62. A method as recited in claim 59, further comprising implementing cluster sub-boundaries to restrict the ability of computers within a cluster to communicate with other computers within the cluster.

63. A method comprising:

generating, at a computer, a landlord key pair and a tenant key pair, each key pair including a private key and a public key, the landlord key pair being used to establish secure communication between the computer and a landlord device, and the tenant key pair being used to establish secure communication between the computer and a tenant device;

keeping the landlord private key and the tenant private key secure at the computer without disclosing the keys to any other device;

forwarding the landlord public key and the tenant public key to the landlord device; and

forwarding the tenant public key to the tenant device.

64. A method as recited in claim 63, further comprising generating a storage key to encrypt data to be stored on a mass storage device.

65. A method as recited in claim 64, further comprising discarding the current storage key each time the tenant private key is changed, and generating a new storage key.

66. A method as recited in claim 64, wherein the generating the storage key comprises combining a landlord symmetric key and a tenant symmetric key to generate the storage key.

67. A method as recited in claim 63, further comprising forwarding the tenant key to the tenant device via the landlord device.

68. A method as recited in claim 63, wherein the landlord device comprises a cluster operations management console.

69. A method as recited in claim 63, wherein the tenant device comprises an application operations management console.

70. A method comprising:

maintaining, at a computer, a storage key to encrypt data to be stored on a mass storage device;

using, as the storage key, only a landlord key if no tenant key has been generated at the computer; and

if a tenant key has been generated at the computer, then combining the landlord key and the tenant key to generate the storage key.

71. A method as recited in claim 70, further comprising combining the landlord key and the tenant key by using the landlord key to encrypt the tenant key.

72. A method as recited in claim 70, further comprising combining the landlord key and the tenant key by using the tenant key to encrypt the landlord key.

73. A multi-tiered computer management architecture comprising:

a first tier corresponding to an owner of a computer;

a second tier corresponding to a hardware operator that is to manage hardware operations of the computer;

a third tier corresponding to a software operator that is to manage software operations of the computer; and

a fourth tier corresponding to the owner, wherein the owner operates in the fourth tier except when revoking the rights of the hardware operator or software operator.

74. An architecture as recited in claim 73, wherein the second tier management is implemented at a management console at a location remote from the computer.

75. An architecture as recited in claim 73, wherein the third tier management is implemented at a management console at a location remote from the computer.

76. An architecture as recited in claim 73, further comprising using a plurality key pairs, each key pair including a private key and a public key, to securely communicate between the computer and a management device corresponding to the hardware operator, as well as between the computer and a management device corresponding to the software operator.